What COVID-19 Taught Us About Cyber Risk

VGM Insurance SERVICES

800.362.3363 | info@vgminsurance.com

The COVID-19 pandemic created challenges in every corner of every industry across the globe—but it taught us as much as it challenged us, and businesses have learned how resilient and adaptable they are. Many organizations found themselves acclimating to a remote work landscape that will never be the same.

Yet, just as businesses scrambled to get their workers and customers online, they then scrambled to protect themselves from increased cybersecurity threats. Ransomware attacks—a form of malware that effectively holds a computer system or its data hostage—which were already increasing in frequency, surged as the pandemic hit. According to VMWare Carbon Black—a company offering endpoint protection services—ransomware attacks it monitored jumped 148% in March 2020 compared to February.

What's been true before still holds true now—the easiest way for a hacker to infiltrate your company is through your people. In a remote work landscape, the security provided by an in-office network can quickly disintegrate, making it more important than ever to educate your staff on proper security measures. As you continue to adapt and provide flexibility to your employees and customers, here are some lessons to keep in mind.

Phishing: Old Reliable

Phishing attacks have long been a staple among cyber criminals' tactics. These are attempts from hackers to trick an individual into divulging sensitive information about themselves or a company that would help them gain access to a computer system. The COVID-19 pandemic, however, gave rise to hackers disguising themselves as charitable organizations.

Often, attacks take the form of an email, but can also be a text message, social media message or post, and even a phone call. To help keep you safe, here are eight tips that could save you from falling victim to a phishing attack.

8 Tips to Avoid Phishing Attacks

1. Verify the sender's email address. Look closely and search for previous conversations with the entity to confirm the address is legitimate.
2. Look for spelling and grammar errors. Phishing attacks are frequently full of mistakes.
3. Keep your information to yourself. Most legitimate companies avoid asking for sensitive information over email or text. It's best to provide this through a secure site or over the phone (provided you initiated the call).
4. Be wary of urgent messages. Hackers try to put pressure on victims in this way to increase their chance of success.
5. Call to get verification. If you're unsure of a request made over email or text, call the source directly.
6. Don't open attachments you didn't ask for. These can carry embedded malware, so it's best not to open them.
7. Check hyperlinks before you click. Hover over hyperlinked text to view the web address and ensure it's legitimate before clicking on it.
8. Contact your IT or security team. When in doubt about a message's validity, report it to your IT or security team to have them verify it.

Spear Phishing: A More Targeted Approach

Spear phishing is a more sophisticated attack where—instead of posing as an organization—hackers attempt to pose as a colleague or someone you trust to deceive you into relinquishing sensitive information.

They do their research, looking for information online about you and people you know. And the more they know, the easier it is for them to trick you into opening an attachment or clicking a link. You're not powerless, though. Here are eight tips to help keep you safe from a spear phishing attack.

8 Tips to Avoid Spear Phishing Attacks

1. Never send financial or personal information electronically, even if you know the recipient well. A third party could intercept this information.
2. Be cautious when asked for personal information in an email. Even if it appears to be from a trusted source, it could be a hacker impersonating another person or group.
3. Only share personal information on secure websites or over the phone. You can ensure a website is secure when you see a lock icon in the URL bar, or when an "s" is present in the "https" of a URL. The "s" stands for "secure" at the end of the normal "http." And only share information over the phone if you initiate the call to a trusted number.
4. Never click on links or open attachments from unknown sources. Even opening a file that seems familiar can give a spear phishing attacker access to personal information.
5. Keep security software up to date. Firewalls and antivirus software can help protect against spear phishing attacks.
6. Think twice about what is posted online. Spear phishing hackers often obtain personal information through social media sites. Educate employees on how to keep information private to protect their own security and that of your business.
7. Regularly check online accounts and bank statements to ensure no one has accessed them without authorization.
8. Never enter any personal or financial information into a pop-up window or a web browser.

What Can Employers Do?

Despite the persistence of hackers, there are steps you can take to help protect yourself from cybersecurity threats. Here are five steps you can take:

5 Steps to Protect Your Business From Cybersecurity Threats

1. Keep employees informed of known cybersecurity threats. When your IT or security team learn of a new attack making the rounds, they should inform the company to be on alert and indicate what they can watch for.
2. Educate employees on security best practices. Start with the best practices listed above for phishing and spear phishing, but don't stop there. Many companies have contracted with third-party organizations to supply ongoing cybersecurity training.

3. Create cybersecurity policies and hold employees accountable. A good policy should:

    a. Ensure employees are using the company's virtual private network (VPN) to access company systems and data when working remotely.

    b. Mandate the use of security and antivirus software that is kept up to date and includes the latest patches.

    c. Outline the kinds of sensitive data employees are obligated to protect (e.g., confidential business information, trade secrets, intellectual property, and personal information.)

    d. Prohibit employees from sharing their work devices with friends and family members.

    e. Establish a process that employees can use to report lost or stolen equipment. This will help your IT department respond quickly and mitigate potential data loss threats.

    f. Require two-factor authentication for all company passwords, adding a layer of security to prevent credentials from being compromised.

    g. Consider security precautions for mobile devices. Depending on how your organization uses such devices, unauthorized access to the information on a smartphone or tablet could be just as damaging as a data breach involving more traditional computer systems.

4. Back up data and strengthen network protections. Strengthening network protections can help prevent an attack from penetrating your systems. In the event something gets through, however, it's best to have a backup of your data in case you need to revert back to it following a ransomware attack.

5. Talk to your insurance agent or broker. Insurance agents and brokers are in the business of keeping you safe. Be sure to review your current coverage to ensure you're adequately protected and have the proper Cyber Liability coverage in place. Your insurance provider is also a great resource for best practices to help you prevent an attack from happening.

For more information about how you can manage the risks associated with cybersecurity threats in your business and to ensure you have adequate coverage, reach out to your VGM Insurance Services Account Manager or contact us today at info@vgminsurance.com or 800-362-3363.

VGM Insurance SERVICES